REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between City of Waukesha's networks and untrusted networks, as well as traffic into and out of more sensitive areas within City of Waukesha's internal trusted networks. The Cardholder Data Environment (CDE) is an example of a more sensitive area within City of Waukesha's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in PCI DSS Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of PCI DSS Requirement 1.

PCI DSS CONTROL 1.1

Control Objective: The organization establishes firewall and router configuration standards that follow industry-recognized leading practices.

Standard: Asset custodians are required to establish firewall and router configuration processes that include the following:[3]

(a) Asset custodians are required to establish and maintaining a formal process for approving and testing all network connections and changes to both firewall and router configurations;[4]

(b) Asset custodians are required to establish and maintaining detailed network diagrams. Network diagrams must:[5]
   1. Document all connections to cardholder data, including any wireless networks;
   2. Be reviewed annually; and
   3. Be updated as the network changes to reflect the current architecture in place;

(c) Asset custodians are required to establish and maintaining detailed data flow diagrams that show all cardholder data flows across systems and networks; A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and City of Waukesha's internal networks;[6]

(d) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes;[7]

(e) A documented business justification is required for all services, protocols, ~~and~~ ports, and applications allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure;[8] and

(f) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover:[9]
   1. Validation of Access Control Lists (ACLs); and
   2. Vulnerability management (e.g., validating software and firmware is current).

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Internet Message Access Protocol (IMAP)

Procedures: Firewall rules are reviewed quarterly. All major changes follow Change Management procedures.

[3] PCI DSS v3.2 Requirement 1.1
[4] PCI DSS v3.2 Requirement 1.1.1
[5] PCI DSS v3.2 Requirement 1.1.2
[6] PCI DSS v3.2 Requirement 1.1.4
[7] PCI DSS v3.2 Requirement 1.1.5
[8] PCI DSS v3.2 Requirement 1.1.6
[9] PCI DSS v3.2 Requirement 1.1.7

PCI DSS CONTROL 1.2

Control Objective: The organization builds firewall and router configurations that restrict connections between untrusted networks and any system components in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to deploy and configure of firewalls and routers in order to restrict connections between untrusted networks and any system components within the Cardholder Data Environment (CDE) by the following means: [10]

(a) Implementing Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to the CDE to only that which is necessary, as defined by a business justification; [11]
(b) Securing and synchronizing router and firewall configuration files; [12] and
(c) Positioning perimeter firewalls between wireless networks and the CDE.[13]

PCI DSS CONTROL 1.3

Control Objective: The organization prohibits direct public access to the Internet and any system component in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to establish and manage firewall and router configuration standards to prohibit direct public access to the Internet and any system component in the Cardholder Data Environment (CDE) that includes, but is not limited to: [14]

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [15]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [16]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [17]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [18]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [19]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [20] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [21]

Supplemental Guidance: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated so that filtering decisions would not only be based on administrator-defined rules, but also on the context that has been built by previous connections as well as previous packets belonging to the same connection.

[10] PCI DSS v3.2 Requirement 1.2
[11] PCI DSS v3.2 Requirement 1.2.1
[12] PCI DSS v3.2 Requirement 1.2.2
[13] PCI DSS v3.2 Requirement 1.2.3
[14] PCI DSS v3.2 Requirement 1.3
[15] PCI DSS v3.2 Requirement 1.3.1
[16] PCI DSS v3.2 Requirement 1.3.2
[17] PCI DSS v3.2 Requirement 1.3.3
[18] PCI DSS v3.2 Requirement 1.3.4
[19] PCI DSS v3.2 Requirement 1.3.5
[20] PCI DSS v3.2 Requirement 1.3.6
[21] PCI DSS v3.2 Requirement 1.3.7

Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls,
- Removal or filtering of route advertisements for private networks that employ registered addressing, or
- Internal use of RFC1918 address space instead of registered addresses.

PCI DSS CONTROL 1.4

Control Objective: The organization installs personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.

Standard: Asset custodians are required to install and maintain firewall software or equivalent functionality on any Internet-accessible mobile device or computer which are used to access the Cardholder Data Environment (CDE) that includes, but is not limited to: [22]

(a) Firewall software must be configured by City of Waukesha's IT department;
(b) Configuration settings of the firewall software must not be alterable by standard users; and
(c) Firewall configurations must include:
    1. Specific configuration settings are defined for firewall software.
    2. Firewall software is actively running.
    3. Firewall software is not alterable by users of mobile devices and/or computers.

Supplemental Guidance: Examples of mobile devices and computers includes, but are not limited to:

- Laptops
- Tablets
- Smart phones

Procedures: The City uses NG Antivirus protection, which contains firewall rules and also works directly with the City's firewall.

PCI DSS CONTROL 1.5

Control Objective: Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for managing firewalls are kept current and disseminated to all pertinent parties. [23]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Procedures: The City IT department has a documentation Wiki where polices and procedures are stored.

[22] PCI DSS v3.2 Requirement 1.4
[23] PCI DSS v3.2 Requirement 1.5

REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS

Malicious individuals (external and internal to an organization) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and are easily determined via public information.

PCI DSS CONTROL 2.1

Control Objective: The organization always changes vendor-supplied defaults before installing a system on the network.

Standard: Asset custodians are required to ensure vendor-supplied defaults are changed, prior to the information system being installed on the network. This pre-production hardening process for both wired and wireless information systems must include, but is not limited to: [24]

(a) Changing vendor default credentials: [25]
    1. Passwords;
    2. Simple Network Management Protocol (SNMP) community strings; and
    3. Encryption keys
(b) Disabling or deleting unnecessary accounts;
(c) Updating firmware on devices; and
(d) Verifying other security-related vendor defaults are changed, if applicable.

Supplemental Guidance: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.) Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.

Procedures: This is a standard procedure.

PCI DSS CONTROL 2.2

Control Objective: The organization develops configuration standards for all system components that are consistent with industry-accepted system hardening standards.

Standard: Asset custodians are required to develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to: [26]

(a) Verifying that system configuration standards are:
    1. Updated as new vulnerability issues are identified;
    2. Applied when new systems are configured;
    3. Consistent with industry-accepted hardening standards;
(b) Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers); [27]
(c) Enforcing least functionality, which includes but is not limited to:
    1. Allowing only necessary and secure services, protocols, and daemons; [28]
    2. Removing all unnecessary functionality, which includes but is not limited to: [29]
        i. Scripts;
        ii. Drivers;
        iii. Features;
        iv. Subsystems;
        v. File systems; and
        vi. Unnecessary web servers
(d) Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH) v2 and higher, Secure File Transfer

[24] PCI DSS v3.2 Requirement 2.1
[25] PCI DSS v3.2 Requirement 2.1.1
[26] PCI DSS v3.2 Requirement 2.2
[27] PCI DSS v3.2 Requirement 2.2.1
[28] PCI DSS v3.2 Requirement 2.2.2
[29] PCI DSS v3.2 Requirement 2.2.5

Protocol (S-FTP), Transport Layer Security (TLS) v1.2 and higher, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP; [30]

(e) Verifying system security parameters are configured to prevent misuse; [31] and

(f) Documenting the functionality present on information systems.

Supplemental Guidance: Appendix J: System Hardening contains the approved baseline configurations. Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Cybersecurity Agency (DISA) Security Technical Implementation Guides (STIGs) [32]

If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS Control 2.3

Control Objective: The organization encrypts all non-console administrative access using strong cryptography.

Standard: Asset custodians are responsible for developing configuration standards to ensure all non-console administrative access is encrypting using strong cryptography using technologies such as SSH v2 and higher, VPN, or TLS v1.2 and higher for web-based management and other non-console administrative access. [33]

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP);
- Telnet; and
- Post Office Protocol 3 (POP3).

Procedures: SSH v2 and higher, and TLS v1.2 and higher are the standards used by City IT.

PCI DSS Control 2.4

Control Objective: The organization maintains an inventory of system components that are in scope for PCI DSS.

Standard: Asset custodians are required to maintain an inventory of City of Waukesha's information systems that are in scope for PCI DSS and update the inventory at necessary. [34]

Supplemental Guidance: Maintaining a current list of all system components will enable City of Waukesha to accurately and efficiently define the scope of its CDE for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from applicable configuration standards.

Procedures: The inventory is maintained in our CMDB.

PCI DSS Control 2.5

Control Objective: The organization ensures that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for managing vendor defaults and other security parameters are kept current and disseminated to all pertinent parties. [35]

[30] PCI DSS v3.2 Requirement 2.2.3
[31] PCI DSS v3.2 Requirement 2.2.4
[32] DISA STIGs official site: http://iase.disa.mil/stigs/index.html
[33] PCI DSS v3.2 Requirement 2.3
[34] PCI DSS v3.2 Requirement 2.4
[35] PCI DSS v3.2 Requirement 2.5

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

Procedures: This is standard practice.

PCI DSS CONTROL 2.6

Control Objective: The organization's shared hosting providers protect the organization's hosted environment and cardholder data.

Standard: For shared hosting providers, City of Waukesha's contract owners, asset custodians and data owners are required to: [36]

(a) Maintain a comprehensive list of those service providers, including all applicable Service Level Agreements (SLAs);
(b) Require that providers of external information systems comply with City of Waukesha cybersecurity requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements (e.g., PCI DSS);
(c) Define oversight responsibilities with regard to external information system services;
(d) Perform a review of the service provided for acceptable service levels;
(e) Conduct a risk assessment outsourcing of services; and
(f) Monitor security control compliance by those external service providers.

Supplemental Guidance: These providers must meet specific requirements as detailed in Appendix A (Additional PCI DSS Requirements for Shared Hosting Provider) of the PCI DSS.

Procedures: The City requires all hosting providers to provide their documentation annually.

[36] PCI DSS v3.2 Requirement 2.6